R&S®SITLine ETH: Securing rail control networks

You act. We protect.
Encryption & IT security
by Rohde & Schwarz SIT.

ROHDE&SCHWARZ

Contents

Rail operations are supervised by operations centers, which manage actuated equipment such as barriers, signals and switches via control and monitoring networks. These control networks are protected by a range of safety measures designed to guard against faults and minimize technical risks. However, they also need security provisions in place to protect them from deliberate manipulation. The R&S®SITLine ETH family of products provides cryptographic functionality to secure the data traffic on control networks.

Products from Rohde&Schwarz

- R&S®SITLine ETH50
  Ethernet encryptor for 25 Mbit/s to 100 Mbit/s
- R&S®SITLine ETH100
  Ethernet encryptor for 4 × 100 Mbit/s
- R&S®SITLine ETH1G
  Ethernet encryptor for 1 Gbit/s
- R&S®SITScope
  security management system

Safety and security 3
1.1 Technical system safety 3
1.1.1 Reliability and availability 3
1.1.2 Isolation 4
1.2 Security against human factors 4
1.2.1 Avoiding operator error 4
1.2.2 Resilience to attack 4

The rail control and monitoring network 5
2.1 Connecting the operations center and the track 5
2.1.1 At the heart of the control zone: the control and monitoring network 5
2.1.2 Safety in a flat network 5
2.1.3 An Achilles' heel: man-in-the-middle vulnerability 5
2.1.4 Adding security with the R&S®SITLine ETH50 6
2.2 Control network management 6
2.2.1 Management centers 6
2.2.2 Safety through multiple redundancy 6
2.2.3 The threat to operations control 6
2.2.4 The R&S®SITLine ETH100 and R&S®SITLine ETH1G: high-performance encryptors 7

R&S®SITLine ETH encryptors – a product and a solution in one 8
3.1 A single solution for operations and management centers 8
3.1.1 A unified management system 8
3.1.2 A cost-effective spare parts inventory 8
3.1.3 Reduced complexity 8
3.2 Confidentiality and integrity protection in a single product 9
3.2.1 Dedicated network security 9
3.2.2 Security based on approved cryptography 9
3.2.3 Integrity and confidentiality protection 9

Ordering information 10

Safety and security

Rail networks are one of society's most critical infrastructures. Their ability to operate smoothly at all times is in everyone's interest – politically, economically and individually. Even minor problems can rapidly have wider negative impacts on a major scale. Disruptions to rail services impede the flow of goods and prevent people from starting work on time – both of which can affect business processes. Malfunctions that cause damage to materials or harm to people are disastrous and must be prevented.

Malfunctions are usually the result of technical failures or human intervention. Potential technical risks include defects and interference radiation. Efforts directed at minimizing these technical risks are referred to generally as safety measures. Security measures, by contrast, encompass efforts to prevent disruptions resulting from deliberate attacks and unintentional human interference.

1.1 Technical system safety

In control and monitoring networks, safety measures focus on ensuring network reliability and availability and guarding against mutual interference.

1.1.1 Reliability and availability

Two fundamental measures aim to provide reliability and availability:

- Single or multiple redundancy of devices and transmission paths
- Reduction of IT system complexity

Redundancy can be added at various points in a system: The options include parallel transmission paths, redundant power feeds and full device redundancy. Each such measure requires functionality for monitoring, reporting and, where appropriate, automated switching.

Complexity can be reduced early on, at the system design stage, by selecting suitable technologies. Two independent data communications cables, for instance, offer a much greater degree of protection than two separate communications channels running over the Internet. The latter generally involve greater complexity because of the large number of applications, users and network carriers, and the related dependencies. Fewer “players” means less dependency and lower overall system complexity.

Throwing the wrong switch or setting the wrong signals can have severe consequences, including loss of human life. This means that simply increasing the reliability of trains or continuously improving their resilience to technical faults is not enough. The IT communications networks that control and monitor a rail network must also meet tough requirements in terms of information path availability and reliability, and data integrity.

1.1.2 Isolation

Communications relationships in IT systems are considered isolated if faults that occur in them will not have a knock-on effect on other (adjacent) communications relationships. This does not apply solely to faults: Functionality, too, must not be allowed to have an impact on the transmission of information.

Optimum protection against interference can be achieved in IT communications networks if they are planned from the outset with as few users per communications segment as possible. Ideally, no more than two users should ever be connected with one another. If this is the case, a malfunction experienced by one user will only affect one other, directly connected user. This approach allows effective error containment and simplifies the troubleshooting process.

1.2 Security against human factors

The purpose of security measures is to guard systems against faults caused either unintentionally or deliberately by people. These measures also extend to the avoidance of operator error and the implementation of resilience to attack.

1.2.1 Avoiding operator error

Unintentional errors can be avoided through a combination of technical monitoring (plausibility checks on inputs) and employee training. Critical operator tasks need to be audit-proofed – by requiring a digital signature, for example. In highly sensitive areas, systems may require more than one properly authenticated individual to be present for certain types of inputs (mutual supervision).

1.2.2 Resilience to attack

Random transmission errors and the changes they cause in the information sent can be identified and corrected to a certain extent using common mechanisms such as CRC checksums and Reed-Solomon error correction. However, these methods fail when faced with a deliberate attack. Only cryptographic mechanisms afford protection against this kind of threat. The methods available are:

- Encryption to protect confidentiality
- Data integrity protection to guard against manipulation and random transmission errors
- Authentication to identify replay attacks

Because these cryptographic mechanisms are built into the network, they must comply with safety requirements (see section 1.1).

R&S®SITLine ETH devices protect communications in critical infrastructure.

The rail control and monitoring network

2.1 Connecting the operations center and the track

2.1.1 At the heart of the control zone: the control and monitoring network

The rail network is divided up into control zones for the purpose of monitoring rail traffic. Each zone covers several sections of track. The control zones are managed by a regional operations center. In the operations center, the train director uses a special control and monitoring network to release individual routes in each of the control zones (by switching the traction current and setting signals, for example).

The control and monitoring network connects the operations center with actuated trackside equipment such as barriers. Connections of this type run over public networks, linking train stations and interlockings, both of which function as subcenters. The subcenters control communications to and from trackside distribution cabinets. These latter connections run over the rail operator's own infrastructure or public networks, depending on availability. From the distribution cabinets, communications run on separate lines along the tracks, to the signals, axle counters and switches.

2.1.2 Safety in a flat network

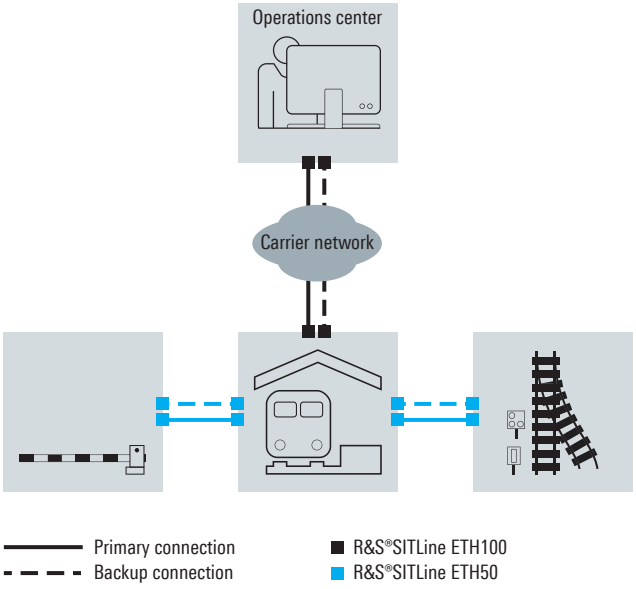
To keep complexity down, the control and monitoring network is a flat network that primarily uses switches, and only a few routers. The control information (the rail system service data) consists of small data packets between 60 bytes and 100 bytes long. The operations control applications incorporate functions that use checksums to identify random transmission errors.

Every communications link is redundant. If one line fails, communications run over the backup line. The switchover time is minimal. The redundancy on links connecting actuated equipment consists of redundant star or ring cabling topology. If a communications link over ring cabling is interrupted, a backup connection in the opposite direction is available. All of the links are implemented as point-to-point connections to prevent cross-interference.

2.1.3 An Achilles' heel: man-in-the-middle vulnerability

Potential attackers able to access the control and monitoring network can manipulate data transmissions. They might access the network physically (through unprotected lines, network nodes or distribution points, for instance) or remotely, over the public network. After a brief analysis of the application protocol, attackers could manipulate data and then retransmit it, complete with correct, recomputed checksums. This means it would be possible for a man-in-the-middle attack to go unnoticed. Cryptographic security functions can protect applications against attacks of this kind.

Monitoring sections of track



The sections of track in a control zone are monitored by a regional operations center.

2.1.4 Adding security with the R&S®SITLine ETH50

The R&S®SITLine ETH50 encryptor can add the necessary security to rail control and monitoring networks. Designed to be mounted on a top-hat rail (DIN rail), it has an extended operating temperature range from –20 °C to +70 °C, making it suitable for installation either in a trackside cabinet or in an air-conditioned data center. Its long operating life and remote control capability mean exceptionally low operating costs, even when deployed in a geographically dispersed network. The mean operating life is specified at 350 000 hours – in other words, more than 30 years. Rohde&Schwarz takes extensive measures to ensure the long-term availability of its products and spare parts.

2.2 Control network management

2.2.1 Management centers

The control and monitoring networks are supervised from two management centers. These centers not only evaluate status messages received from network and security components, they are also responsible for granting permissions and controlling access. For example, one of the centers runs the root CA for the corporate PKI, generating device and user certificates securely.

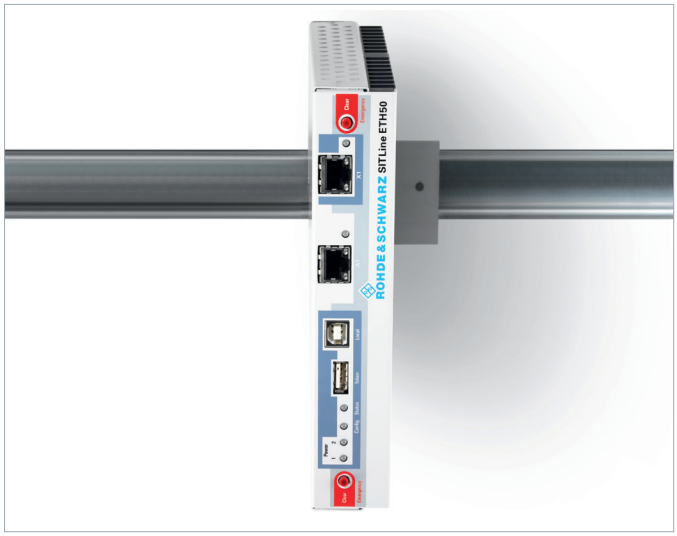
2.2.2 Safety through multiple redundancy

The management centers are at separate sites for geographic redundancy. Both also have redundant network connectivity. Connections between the two management centers and the operations centers go a stage further and are multiply redundant. Each operations center has two network links, both of which can connect to the two management centers. The network links and related devices run in active/passive mode to allow a rapid switchover if the primary link fails. With this setup, primary and backup connections between an operations center and both management centers are available.

2.2.3 The threat to operations control

Connecting operations centers inexpensively over public networks exposes them to potential attacks on control and monitoring network integrity and poses a threat to rail operations. Although rail operations are completely under the operations centers' control, status messages and other management data can be intercepted and manipulated nonetheless. This means it is impossible to ensure the authenticity of the data. To properly safeguard the integrity of the data, it needs to be encrypted.

The R&S®SITLine ETH50 can be installed in distribution cabinets on a top-hat rail (DIN rail).



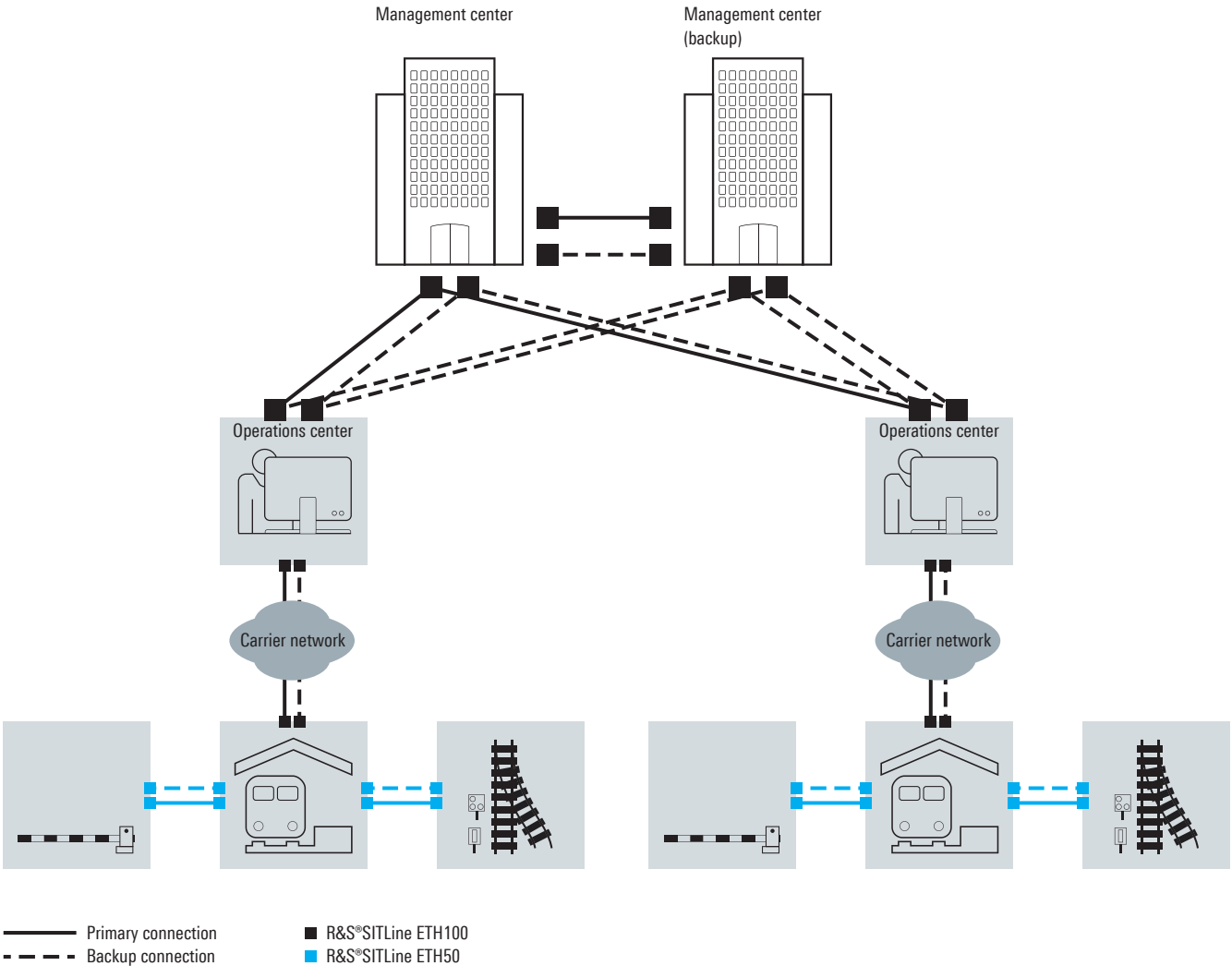
2.2.4 The R&S®SITLine ETH100 and R&S®SITLine ETH1G: high-performance encryptors

R&S®SITLine ETH100 and R&S®SITLine ETH1G deliver security without noticeably increasing the operating costs. These devices combine a compact form factor (19", 1 HU) and low space requirements with minimal power consumption. They use cipher feedback mode (CFB), which provides security without adding protocol overhead (a zero overhead option). The encryption on the transmission layer (layer 2, Ethernet) also secures the significantly more complex protocols running on top of it. This prevents attacks such as UDP flooding, TCP hijacking and DNS spoofing on the transmission network.

R&S®SITLine ETH100 and R&S®SITLine ETH1G encryptors are intended specifically for high-availability data centers. Designed for fault tolerance, they all have redundant power supplies; the multiport devices are additionally equipped with redundant transceivers. Under ordinary circumstances, the encryptors can operate without relying on central network components such as key servers. Capable of supporting up to 4000 secure connections per device, R&S®SITLine ETH100 and R&S®SITLine ETH1G encryptors are a safe investment in terms of future network expansion.

With R&S®SITLine ETH devices, users can switch from IPv4 to IPv6 when they need to – easily and without incurring additional costs for security.

Management centers



R&S®SITLine ETH encryptors – a product and a solution in one

3.1 A single solution for operations and management centers

R&S®SITLine ETH is a family of Ethernet encryptors. All of the products in the family can be used in combination with one another, both cryptographically and in terms of networking. The full range of security functionality they offer has been implemented consistently across all device models. They also share the same security certification.

3.1.1 A unified management system

The devices deployed in the operations and management centers are all configured and operated using the same security management system, R&S®SITScope. Consistent user interaction across all models helps reduce errors caused by different users working on different systems. In addition, users can acquire all the knowledge they need in a single training course.

3.1.2 A cost-effective spare parts inventory

Devices in the product family share components such as transceivers, batteries and power supplies. This simplifies servicing and reduces costs.

3.1.3 Reduced complexity

Deploying a unified and homogeneous solution improves system availability and stability. It also simplifies upgrade and recertification processes (change management).

The same security functionality is available across all device variants designed for different environmental specifications. This gives users flexibility in planning data center and trackside security without increasing complexity.

The R&S®SITLine ETH50, measuring 7.5", is intended for trackside deployment, whereas the R&S®SITLine ETH100 is a 19" unit designed to be installed in a data center. Both devices have a 1 HU form factor.

3.2 Confidentiality and integrity protection in a single product

R&S®SITLine ETH encryptors deliver the requisite security without compromising safety.

3.2.1 Dedicated network security

Cryptographic functionality is compute-intensive and generates a high CPU load. Dedicated encryption devices ease the workload on active network components by taking care of this for them. This leaves more system resources available for tasks such as routing and switching, and reduces the risk of security-related interference, particularly when network load peaks. In addition, a clear separation between network functionality and security allows security to be managed separately by security officers or administrators.

R&S®SITLine ETH encryptors secure individual point-to-point connections with dedicated session keys. Encryption has no effect on traffic profiles because the kind implemented in R&S®SITLine ETH devices is free of overhead. Data volumes and responsiveness remain in an acceptable range.

Redundancy requirements can be met in full by deploying separate encryptors, without impacting on switching times. The R&S®SITLine ETH devices themselves are fitted with redundant power supplies.

3.2.2 Security based on approved cryptography

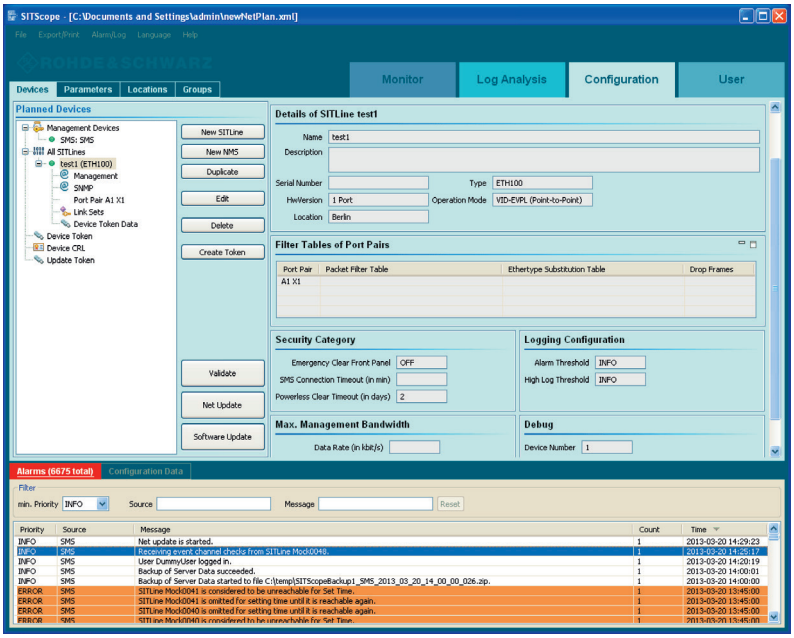
The R&S®SITLine ETH family of encryptors was developed by Rohde&Schwarz SIT GmbH, which specializes in IT security. The algorithms and key lengths used for encryption and integrity protection are constantly being refined to address the latest threats. The devices are equipped with a smart card for generating secure keys. This smart card is certified to Common Criteria EAL4+.

R&S®SITLine ETH devices are also protected thoroughly against physical tampering. They can detect attempts to open them and, depending on the chosen configuration, will trigger an emergency erasure of their own key material. The devices have LEDs that reliably indicate the current operating mode – encrypted or clear.

3.2.3 Integrity and confidentiality protection

R&S®SITLine ETH encryptors protect the integrity and confidentiality of data. The integrity protection they provide guards network connections against replay attacks and the deliberate manipulation of control information (even if CRC checksums are recalculated). Encryption ensures that the data transmitted remains confidential. As a further level of integrity protection, the encryption functionality also requires strong authentication.

R&S®SITScope ETH: unified security management system for R&S®SITLine ETH devices.



Ordering information

Designation	Type	Order No.
R&S®SITLine ETH50, half-rack format (7.5"), 1 HU		
Ethernet Encryptor, 1 line, 25 Mbit/s	R&S®SITLine ETH50-25	5401.8830K02
Ethernet Encryptor, 1 line, 50 Mbit/s	R&S®SITLine ETH50-50	5401.8830K02
Ethernet Encryptor, 1 line, 100 Mbit/s	R&S®SITLine ETH50-100	5401.8830K02
R&S®SITLine ETH100, rack format (19"), 1 HU		
Ethernet Encryptor, 1 line, 100 Mbit/s	R&S®SITLine ETH100-110	5401.7004K11
Ethernet Encryptor, 2 lines, 100 Mbit/s	R&S®SITLine ETH100-210	5401.7004K12
Ethernet Encryptor, 4 lines, 100 Mbit/s	R&S®SITLine ETH100-410	5401.7004K13
R&S®SITLine ETH1G, rack format (19"), 1 HU		
Ethernet Encryptor, 1 line, 1 Gbit/s	R&S®SITLine ETH1G-110	5401.6820K11
R&S®SITLine device token (one token required per device)		
Device token, USB/smart card		5410.0650.04
R&S®SITScope, security management		
Set consisting of software and tools on CD (server and client software, R&S®SITLine Admin, R&S®SITLine Terminal), USB tokens (3 root tokens, 2 supervisor tokens, 2 manager tokens), USB cable (type A to B)	R&S®SITScope Set	5410.8400K53
R&S®SITScope Set, pre-installed on server hardware	R&S®SITScope Appliance	5410.8400K13
Accessories for R&S®SITLine ETH50		
USB cable (type A to B), for local initialization		1502.0567.00
External power supply for R&S®SITLine ETH50, 110 V to 240 V, 50/60 Hz		5401.8898.00
Accessories for R&S®SITLine ETH100/R&S®SITLine ETH1G		
Electric SFP transceiver (10/100/1000BaseT) for R&S®SITLine ETH100 and R&S®SITLine ETH1G		5401.8198.00
Optical SFP transceiver (1000BaseSX) for R&S®SITLine ETH1G		4055.6412.00
Optical SFP transceiver (1000BaseLX) for R&S®SITLine ETH1G		5401.8181.00
Accessories for R&S®SITScope		
Manager token, USB/smart card		5410.0650.02
Root token, USB/smart card		5410.0650.03
Supervisor token, USB/smart card		5410.0650.05
Manuals		
User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, German		5401.8900.31
User manual, R&S®SITLine ETH50, German		5401.8875.31
User manual, R&S®SITLine ETH100/R&S®SITLine ETH1G, English		5401.8900.32
User manual, R&S®SITLine ETH50, English		5401.8875.32
User manual, R&S®SITScope, German		5410.8439.31
User manual, R&S®SITScope, English		5410.8439.32

Product brochure for R&S®SITLine ETH, see PD 5214.0724.12;
data sheet for R&S®SITLine ETH100/R&S®SITLine ETH1G, see PD 5214.0724.22;
data sheet for R&S®SITLine ETH50, see PD 5214.4607.22;
and www.rohde-schwarz.com

Glossary

Term	Definition
Actuated equipment	In rail systems, equipment such as signals, switches, axle counters and barriers
Certificate	A security certificate confirming by cryptographic means the identity and authenticity of a device or person on a computer network
Certificate authority (CA)	An entity that issues digital certificates
Certification to Common Criteria EAL4+	The Common Criteria are an internationally recognized standard for security evaluation to a given evaluation assurance level
Change management	The process of managing changes in complex systems
Cipher feedback mode (CFB)	A cryptographic mode in which encrypted text has the same scope or length as unencrypted text
Control zone	The sum total of sections of track managed by a single operations center
CRC checksum	Cyclic redundancy check, a checksum-based method that prevents random transmission errors
Data center	A facility that houses an organization's or business customers' data processing and telecommunications systems
DNS spoofing	A form of cyber attack in which an incorrect IP address is mapped to a host name (also called DNS poisoning)
Failover	The process whereby routers and switches switch over to a backup connection in the event that a primary connection fails (supported by R&S®SITLine devices)
Isolation	In communications, a system state whereby a fault in one area will not result in faults in other areas
Management centers	In a corporate network, geographically redundant management sites that monitor network components and provide central security services (PKI)
Man-in-the-middle attack	A cyber attack on a communications link in which attackers insert themselves between two stations in order to read or modify the data traffic
Operations center, train director	Entities responsible for managing rail operations within a control zone
Public key infrastructure (PKI)	A system for creating and distributing security certificates for use by devices and persons
Root CA	A certificate authority that serves as a trust anchor for subordinate CAs
Safety	Technical measures implemented to safeguard the availability, reliability and isolation of a control network
Security	Measures (including cryptographic) to guard against deliberate manipulation and random changes to data
TCP hijacking	A form of cyber attack in which an attacker succeeds in disrupting or taking over a TCP connection (e.g. by successfully guessing the confirmation or response ID for a previously transmitted sequence ID)
Track section	A subsection of a control zone
UDP flooding	A denial-of-service attack using the user datagram protocol

Service you can rely on

- Worldwide
- Local and personalized
- Customized and flexible
- Uncompromising quality
- Long-term dependability

About Rohde&Schwarz

Rohde&Schwarz is an independent group of companies specializing in electronics. It is a leading supplier of solutions in the fields of test and measurement, broadcasting, radiomonitoring and radiolocation, as well as secure communications. Established more than 75 years ago, Rohde&Schwarz has a global presence and a dedicated service network in over 70 countries. Company headquarters are in Munich, Germany.

Environmental commitment

- Energy-efficient products
- Continuous improvement in environmental sustainability
- ISO 14001-certified environmental management system

Certified Quality System
ISO 9001

Rohde&Schwarz SIT GmbH
Am Studio 3 | D-12489 Berlin
Phone +49 30 65884-223 | Fax +49 30 65884-184
E-mail: info.sit@rohde-schwarz.com
www.sit.rohde-schwarz.com

www.rohde-schwarz.com

Regional contact

- Europe, Africa, Middle East | +49 89 4129 12345
  customersupport@rohde-schwarz.com
- North America | 1 888 TEST RSA (1 888 837 87 72)
  customer.support@rsa.rohde-schwarz.com
- Latin America | +1 410 910 79 88
  customersupport.la@rohde-schwarz.com
- Asia/Pacific | +65 65 13 04 88
  customersupport.asia@rohde-schwarz.com
- China | +86 800 810 8228/+86 400 650 5896
  customersupport.china@rohde-schwarz.com

R&S® is a registered trademark of Rohde&Schwarz GmbH&Co. KG
Trade names are trademarks of the owners | Printed in Germany (ch)
PD 3606.6505.92 | Version 01.00 | April 2013 | R&S®SITLine ETH
Data without tolerance limits is not binding | Subject to change
© 2013 Rohde&Schwarz GmbH&Co. KG | 81671 München, Germany

3606650592